

EXPONENTIAL BOUNDS FOR THE ERDŐS-GINZBURG-ZIV CONSTANT

ERIC NASLUND

ABSTRACT. The Erdős-Ginzburg-Ziv constant of an abelian group G , denoted $\mathfrak{s}(G)$, is the smallest $k \in \mathbb{N}$ such that any sequence of length $\mathfrak{s}(G)$ contains a zero-sum subsequence of length $\exp(G)$. In this paper, we use the multi-slice rank method from [12], which is a variant of Tao's slice rank method [15], to prove that

$$\mathfrak{s}(\mathbb{F}_p^n) \leq 3(p-1)p!(J(p)p)^n$$

where $0.8414 < J(p) < .91837$ is a constant depending on p , equal to the constant appearing in Ellenberg and Gijswijt's bounds for arithmetic progression-free subsets in \mathbb{F}_p^n [4]. We also improve upon a recent result of Hegedűs, and show that if $(\mathbb{Z}/k\mathbb{Z})^n$ satisfies *property D* as defined in [7], then

$$\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n) \leq (n-1)\gamma_{k,q}^n + 1$$

where

$$\gamma_{k,q} = \frac{k}{q} \inf_{0 < x < 1} \frac{1-x^q}{1-x} x^{-\frac{q-1}{k}},$$

and q is the largest prime power dividing k . In particular, if $(\mathbb{Z}/q\mathbb{Z})^n$ satisfies property *D* where q is a prime power, then

$$\mathfrak{s}((\mathbb{Z}/q\mathbb{Z})^n) \leq (n-1)4^n + 1.$$

1. INTRODUCTION

For an abelian group G , let $\exp(G)$ denote the exponent of G , which is the maximal order of any element in G . The Erdős-Ginzburg-Ziv constant of G , denoted $\mathfrak{s}(G)$, is defined to be the smallest $k \in \mathbb{N}$ such that any sequence of elements of G of length $\mathfrak{s}(G)$ contains a zero-sum subsequence of length $\exp(G)$. In their original paper, Erdős, Ginzburg and Ziv [5] proved that

$$\mathfrak{s}(\mathbb{Z}/k\mathbb{Z}) = 2k - 1.$$

That is, among any sequence of $2k - 1$ integers there is a subsequence of length k whose sum is divisible by k , and furthermore this is not true if $2k - 1$ is replaced by $2k - 2$. In 2007 Reiher [14] proved that

$$\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^2) = 4k - 3,$$

which resolved a longstanding conjecture of Kemnitz [10], and more generally when $1 \leq k_1 | k_2$,

$$\mathfrak{s}((\mathbb{Z}/k_1\mathbb{Z}) \oplus (\mathbb{Z}/k_2\mathbb{Z})) = 2k_1 + 2k_2 - 3,$$

see [11, Theorem 5.8.3] for a proof. In the case where $G = (\mathbb{Z}/k\mathbb{Z})^n$ with n large, very little is known. Heiko [8] gave the elementary bounds

$$(k-1)2^n + 1 \leq \mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n) \leq (k-1)k^n + 1,$$

and Alon and Dubiner [1] proved that

$$\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n) \leq (cn \log n)^n k$$

for some $c > 0$. Ellenberg and Gijswijt's recent bounds for capsets in \mathbb{F}_3^n [4] imply that

$$\mathfrak{s}((\mathbb{Z}/3\mathbb{Z})^n) \leq 2(J(3)3)^n$$

where

$$J(3) = \frac{1}{8} \sqrt[3]{207 + 33\sqrt{33}} = 0.9183 \dots$$

In this paper, for $p \geq 5$ we give an unconditional exponential improvement to the upper bounds for $\mathfrak{s}(\mathbb{F}_p^n)$ as $n \rightarrow \infty$, where $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z})$ denotes the finite field with p elements. Our main result is:

Theorem 1. *Suppose that $A \subset \mathbb{F}_p^n$ has size*

$$|A| > 3(p-1)p! (J(p)p)^n$$

where

$$J(p) = \frac{1}{p} \inf_{0 < x < 1} \frac{1 - x^p}{(1 - x)x^{2/3}}.$$

Then A contains p distinct elements x_1, \dots, x_p such that

$$x_1 + \dots + x_p = 0.$$

We immediately have the following corollary:

Corollary 1. *The Erdős-Ginzburg-Ziv constant of \mathbb{F}_p^n satisfies*

$$\mathfrak{s}(\mathbb{F}_p^n) \leq 3(p-1)p! (J(p)p)^n.$$

For $p \geq 5$, this implies the bound

$$(1.1) \quad \mathfrak{s}(\mathbb{F}_p^n) \leq (J(p)p)^{n+p},$$

since $3(p-1)p! \leq (J(p)p)^p$ for $p \geq 5$. $J(p)$ is the same constant appearing in Ellenberg and Gijswijt's bound for arithmetic progression-free sets, and in [2, prop. 4.12] it was proven that $J(p)$ is a decreasing function of p , and that

$$\lim_{p \rightarrow \infty} J(p) = \inf_{z > 1} \frac{z - z^{-2}}{3 \log z} = 0.8414 \dots$$

Since $J(3) = 0.9183 \dots$, it follows that for $p \geq 3$, $J(p)$ lies in the range

$$0.8414 \leq J(p) \leq 0.9184.$$

The proof of theorem 1 uses the *multi-slice rank method*, given in [12], which is a variant of *slice rank method* [15]. The multi-slice rank allows us to handle the indicator tensor that results from forcing the variables to be distinct, which has large slice rank for $p \geq 5$. The slice rank method was introduced by Tao [15] following the work of Ellenberg and Gijswijt [4], and the breakthrough result of Croot, Lev and Pach [3]. The slice rank method has seen numerous applications, such as Tao's proof of Ellenberg and Gijswijt's upper bound for progression-free sets in \mathbb{F}_p^n [15, 4], new bounds for the Erdős-Szemerédi sunflower problem [13, 6], and disproving certain conjectures concerning fast matrix multiplication [2]. We refer the reader to [2] for a more detailed discussion of the properties of the slice rank.

We say that a group G satisfies *property D* (see [7, Sec. 7]) if every sequence S of length $\mathfrak{s}(G) - 1$ that does not contain $\exp(G)$ elements summing to 0, when viewed as a multi-set, takes the form

$$S = \cup_{i=1}^{\exp(G)-1} T$$

for some set T . That is, if S is a maximal sequence that does not contain $\exp(G)$ elements summing to zero, then every element in S appears exactly $\exp(G) - 1$ times. Gao and Geroldinger conjecture [7, Conj. 7.2] that $(\mathbb{Z}/k\mathbb{Z})^n$ satisfies property D for every k and n , and under this conjecture we can improve upon the bounds for the Erdős-Ginzburg-Ziv constant using the slice rank method. Recently, Hegedűs [9] showed that if \mathbb{F}_p^n satisfies property D , then

$$\mathfrak{s}(\mathbb{F}_p^n) \leq (p-1)p^{\left(1 - \frac{(p-2)^2}{2p^2 \log p}\right)n+1} + 1,$$

and we give the following improvement:

Theorem 2. *Assume that $(\mathbb{Z}/k\mathbb{Z})^n$ satisfies property D . Then*

$$\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n) \leq (n-1)\gamma_{k,q}^n + 1$$

where

$$\gamma_{k,q} = \frac{k}{q} \inf_{0 < x < 1} \frac{1-x^q}{1-x} x^{-\frac{q-1}{k}}.$$

In particular, if q is a prime power and $(\mathbb{Z}/q\mathbb{Z})^n$ satisfies property D , then

$$\mathfrak{s}((\mathbb{Z}/q\mathbb{Z})^n) \leq (n-1)4^n + 1.$$

Remark 1. When $k = q$ is a prime power, $\gamma_{q,q}$ is at most 4 since

$$\gamma_{q,q} = \frac{q}{q} \inf_{0 < x < 1} \frac{1-x^q}{(1-x)x} x^{-\frac{q-1}{q}} < \inf_{0 < x < 1} \frac{1}{(1-x)x} = 4.$$

For general k, q ,

$$\gamma_{k,q} < \frac{k}{q} \inf_{0 < x < 1} \frac{1}{1-x} x^{-\frac{q-1}{k}} = \frac{k}{q} \left(1 + \frac{q-1}{k}\right) \left(1 + \frac{k}{q-1}\right)^{\frac{q-1}{k}},$$

and as $(1+x)^{\frac{1}{x}}$ is decreasing on $(1, \infty)$, for $k \geq q$ we have the bound

$$\gamma_{k,q} < 2 \left(1 + \frac{k-1}{q}\right).$$

To prove theorem 2, we first prove the following result for subsets of $(\mathbb{Z}/k\mathbb{Z})^n$:

Theorem 3. *Suppose that $A \subset (\mathbb{Z}/k\mathbb{Z})^n$ satisfies*

$$|A| > \gamma_{k,q}^n$$

where

$$\gamma_{k,q} = \frac{k}{q} \inf_{0 < x < 1} \frac{1-x^q}{1-x} x^{-\frac{q-1}{k}},$$

and q is the largest prime power dividing k . Then A contains k not necessarily distinct, but not all equal, elements x_1, \dots, x_k which sum to 0.

Using this result, theorem 2 follows as a corollary.

Proof. (Theorem 3 implies theorem 2) Let S be a sequence in $(\mathbb{Z}/k\mathbb{Z})^n$ of length $\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n) - 1$ for which no k elements that sum to 0. By property D , it follows that as a multi-set

$$S = \cup_{i=1}^{k-1} T$$

for some $T \subset (\mathbb{Z}/k\mathbb{Z})^n$. This implies that the only solution to

$$x_1 + \cdots + x_k = 0$$

for $x_i \in T$ is when $x_1 = x_2 = \cdots = x_k$, and so by theorem 3 $|T| \leq \gamma_k^n$, and hence $\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n) \leq (n-1)\gamma_k^n + 1$. \square

The proof of theorem 3 uses the slice rank method and does not require the multi-slice rank. The key ideas originate in [2], where they extend Ellenberg and Gijswijt's bounds for progression-free sets in \mathbb{F}_p^n to progression-free sets in $(\mathbb{Z}/k\mathbb{Z})^n$ using a binomial coefficient indicator as well as a lemma concerning the slice-rank of a tensor-product. In particular, in [2] they proved the following theorem:

Theorem 4. ([2, Theorem 4.14]) *Suppose that $A \subset (\mathbb{Z}/k\mathbb{Z})^n$ contains no non-trivial 3-term arithmetic progression, that is it contains no non-trivial solutions to the equations $x + y = 2z$. Then*

$$|A| \leq (k \cdot J(q))^n$$

where q is the largest prime power dividing k .

Theorem 3 extends the above result to a k -variable linear equation.

2. THE MULTI-SLICE RANK

To motivate the definition of the slice rank and the multi-slice rank, we begin by recalling the definition of the tensor rank. For finite sets X_1, \dots, X_n , a function

$$h : X_1 \times \cdots \times X_n \rightarrow \mathbb{F},$$

$h \neq 0$, of the form

$$h(x_1, \dots, x_n) = f_1(x_1)f_2(x_2) \cdots f_n(x_n)$$

for some f_1, \dots, f_n , is called a *rank 1 function*, and the tensor rank of

$$F : X_1 \times \cdots \times X_n \rightarrow \mathbb{F}$$

is defined to be the minimal k such that

$$F = \sum_{i=1}^k g_i$$

where the g_i are rank 1 functions. To define the multi-slice rank, we first need some notation. Given variables x_1, \dots, x_n and a set $S \subset \{1, \dots, n\}$, $S = \{s_1, \dots, s_k\}$, let \vec{x}_S denote the k -tuple

$$x_{s_1}, \dots, x_{s_k},$$

and so for a function g of k variables, we have that

$$g(\vec{x}_S) = g(x_{s_1}, \dots, x_{s_k}).$$

Definition 1. Let X_1, \dots, X_n be finite sets. We say that the function

$$h : X_1 \times \dots \times X_n \rightarrow \mathbb{F},$$

$h \neq 0$ is a b -slice for $1 \leq b \leq \frac{n}{2}$ if

$$h(x_1, \dots, x_n) = f(\vec{x}_S)g(\vec{x}_{\{1, \dots, n\} \setminus S})$$

for some f, g and $S \subset \{1, 2, \dots, n\}$ of size $|S| = b$. More generally, we say that F is a *slice* if it is a b -slice for some $1 \leq b \leq \frac{n}{2}$.

For example, the function

$$F : X \times X \times X \times X \rightarrow \mathbb{F}$$

defined by

$$F(x, y, z, w) = \begin{cases} 1 & \text{if } x = y \text{ and } z = w \\ 0 & \text{otherwise} \end{cases}$$

takes the form $F(x, y, z, w) = \delta(x, y)\delta(z, w)$ where $\delta(x, y)$ is 1 if $x = y$, and 0 otherwise, and so F is a 2-slice.

Definition 2. Let X_1, \dots, X_n be finite sets. The *slice rank* of F is the minimal k such that

$$F = \sum_{i=1}^k c_i h_i$$

where each h_i is a 1-slice. The *multi-slice rank* of a function

$$F : X_1 \times \dots \times X_n \rightarrow \mathbb{F}$$

is the minimal k such that

$$F = \sum_{i=1}^k c_i g_i$$

where the g_i are slices, that is each g_i is a b -slice for some $b \leq \frac{n}{2}$.

We note that for two variables, the slice-rank, multi-slice rank and tensor rank are equivalent. For three variables, the multi-slice rank and the slice rank are equivalent, and for 4 or more variables, all three ranks are different. A key property of the multi-slice rank is the following lemma, given in [12, Lemma 8], which generalizes [15, Lemma 1].

Lemma 1. Let X be a finite set, and let X^k denote the k -fold Cartesian product of X with itself. Suppose that

$$F : X^k \rightarrow \mathbb{F}$$

is a diagonal tensor, that is

$$F(x_1, \dots, x_n) = \sum_{a \in A} c_a \delta_a(x_1) \cdots \delta_a(x_n)$$

for some $A \subset X$ where $c_a \neq 0$, and

$$\delta_a(x) = \begin{cases} 1 & x = a \\ 0 & \text{otherwise} \end{cases}.$$

Then

$$\text{multi-slice-rank}(F) = |A|.$$

Proof. See [12, Lemma 8]. \square

The following lemma is proposition 4.2 in [2], and it plays an important role in proving theorem 2.

Lemma 2. *Let G, H be finite abelian groups, and suppose that $u : G^k \rightarrow \mathbb{F}$ and $v : H^k \rightarrow \mathbb{F}$ where G^k denotes the k -fold product $G \times \cdots \times G$. Define the tensor on the product of the groups*

$$u \otimes v : (G \times H)^k \rightarrow \mathbb{F}$$

by writting each element $t \in G \times H$ as a pair $t = (g, h)$ where $g \in G$ and $h \in H$, and setting

$$u \otimes v(t_1, \dots, t_k) = u(g_1, \dots, g_k)v(h_1, \dots, h_k)$$

where t_i is given as the pair (g_i, h_i) for each i . Then

$$\text{slice-rank}(u \otimes v) \leq \text{slice-rank}(u) \cdot |H|.$$

Proof. Suppose that $\text{slice-rank}(u) = k$. Then we may write

$$u(g_1, \dots, g_k) = \sum_{i=1}^k f_i(g_{j_i}) v_i(\vec{\mathcal{G}}_{\{1, \dots, k\} \setminus j_i})$$

for some choice of functions f_i, v_i and indices j_i . For $r_1, \dots, r_k \in H$ we can split v based on its value at each point in H^k and write

$$v(r_1, \dots, r_k) = \sum_{(h_1, \dots, h_k) \in H^k} c_{h_1, \dots, h_k} \delta(h_1, r_1) \cdots \delta(h_k, r_k)$$

where

$$\delta(h, r) = \begin{cases} 1 & \text{if } h = r \\ 0 & \text{otherwise} \end{cases},$$

and $c_{h_1, \dots, h_k} \in \mathbb{F}$ are constants. Then

$$u(g_1, \dots, g_k)v(r_1, \dots, r_k) = \sum_{i=1}^k \sum_{h_{j_i} \in H} f_i(g_{j_i}) \delta(h_{j_i}, r_{j_i}) v_i(\vec{\mathcal{G}}_{\{1, \dots, k\} \setminus j_i}) R(\vec{h}_{\{1, \dots, k\} \setminus j_i})$$

where

$$R(\vec{h}_{\{1, \dots, k\} \setminus j_i}) = \left(\sum_{\vec{h}_{\{1, \dots, k\} \setminus j_i} \in H^{k-1}} c_{h_1, \dots, h_k} \prod_{\substack{l=1 \\ l \neq j_i}}^k \delta(h_l, r_l) \right),$$

and so

$$\text{slice-rank}(u \otimes v) \leq k|H|.$$

\square

3. UNCONDITIONAL BOUNDS FOR $\mathfrak{s}(\mathbb{F}_p^n)$

Let $p > 2$ be a prime number. For $x_1, \dots, x_p \in \mathbb{F}_p^n$, define

$$F_p : (\mathbb{F}_p^n)^p \rightarrow \mathbb{F}_p$$

by

$$(3.1) \quad F_p(x_1, \dots, x_p) = \prod_{i=1}^n (1 - (x_{1i} + x_{2i} + \dots + x_{pi})^{p-1}),$$

where x_{ji} is understood to be the i^{th} coordinate of the vector $x_j \in \mathbb{F}_p^n$, and the notation $(\mathbb{F}_p^n)^p$ is used to denote the p -fold Cartesian product of \mathbb{F}_p^n with itself. Then

$$F_p(x_1, \dots, x_p) = \begin{cases} 1 & \text{if } x_1 + x_2 + \dots + x_p = 0 \\ 0 & \text{otherwise} \end{cases}.$$

This tensor does not take into account whether or not the variables are distinct, and so in particular for any $x \in \mathbb{F}_p^n$

$$F_p(x, \dots, x) = 1.$$

In order to modify this tensor so that it picks up only distinct k -tuples of elements summing to zero, we use the technique in [12], and introduce an indicator which is a sum over the permutations in the symmetric group S_p . For every $\sigma \in S_p$, define

$$(3.2) \quad f_\sigma : X^p \rightarrow \mathbb{F}$$

to be the function that is 1 if (x_1, \dots, x_p) is a fixed point of σ , and 0 otherwise. The following is [12, Lemma 4]:

Lemma 3. *We have the identity*

$$\sum_{\sigma \in S_k} \text{sgn}(\sigma) f_\sigma(x_1, \dots, x_k) = \begin{cases} 1 & \text{if } x_1, \dots, x_k \text{ are distinct} \\ 0 & \text{otherwise} \end{cases},$$

where $\text{sgn}(\sigma)$ is the sign of the permutation.

Proof. By definition,

$$\sum_{\sigma \in S_k} \text{sgn}(\sigma) f_\sigma(x_1, \dots, x_k) = \sum_{\sigma \in \text{Stab}(\vec{x})} \text{sgn}(\sigma)$$

where $\text{Stab}(\vec{x}) \subset S_k$ is the stabilizer of \vec{x} . Since the stabilizer is a product of symmetric groups, this will be non-zero precisely when $\text{Stab}(\vec{x})$ is trivial, and hence x_1, \dots, x_k must be distinct. \square

Using this lemma, we give the following modification of [12, Lemma 5]:

Lemma 4. *Let $C_i \subset S_k$ denote the set all elements in S_k given as a product of i disjoint cycles. Define*

$$R_k(x_1, \dots, x_k) = \sum_{\substack{\sigma \in S_k \\ \sigma \notin C_1, C_2}} \text{sgn}(\sigma) f_\sigma(x_1, \dots, x_k).$$

Then for $k \geq 3$,

$$R_k(x_1, \dots, x_k) = \begin{cases} 1 & \text{if } x_1, \dots, x_k \text{ are distinct} \\ (-1)^{k-1}(k-1)! \sum_{j=2}^{k-1} \frac{1}{j} & \text{if } x_1 = \dots = x_k \\ \alpha(x_1, \dots, x_k) & \text{if } x_1, \dots, x_k \text{ take on 2 distinct values} \\ 0 & \text{otherwise} \end{cases}$$

where

$$\alpha(x_1, \dots, x_k) = (-1)^{k-1} \# \{ \sigma \in \mathcal{C}_2 \text{ that fix } (x_1, \dots, x_k) \}.$$

Proof. If there are 3 or more distinct elements among x_1, \dots, x_k then $f_\sigma(x_1, \dots, x_k) = 0$ for any $\sigma \in \mathcal{C}_2, \mathcal{C}_1$, and so the identity holds by lemma 3. When there are exactly two distinct elements among x_1, \dots, x_k , $f_\sigma(x_1, \dots, x_k) = 0$ for any $\sigma \in \mathcal{C}_1$, and so

$$R_k(x_1, \dots, x_k) = (-1)^{k-1} \# \{ \sigma \in \mathcal{C}_2 \text{ that fix } (x_1, \dots, x_k) \}$$

since $\text{sgn}(\sigma) = (-1)^k$ for any $\sigma \in \mathcal{C}_2$. Lastly, when $x_1 = \dots = x_k$, we have that

$$R_k(x_1, \dots, x_k) + (-1)^k |\mathcal{C}_2| + (-1)^{k-1} |\mathcal{C}_1| = 0$$

by lemma 3 since $\text{sgn } \sigma = (-1)^{k-1}$ for $\sigma \in \mathcal{C}_1$. Since

$$|\mathcal{C}_1| = (k-1)! \quad \text{and} \quad |\mathcal{C}_2| = (k-1)! \sum_{j=1}^{k-1} \frac{1}{j},$$

it follows that

$$R_l(x_1, \dots, x_k) = (-1)^{k-1} \sum_{j=2}^{k-1} \frac{1}{j}$$

when $x_1 = \dots = x_k$. □

Remark 2. Let

$$\delta(x_1, \dots, x_k) = \begin{cases} 1 & x_1 = \dots = x_k \\ 0 & \text{otherwise} \end{cases}.$$

We can calculate $R_k(x_1, \dots, x_k)$ exactly as a linear combination of $k! - (k-1)! - (k-1)! \sum_{j=1}^{k-1} \frac{1}{j}$ delta functions, including the constant function. When $k = 3$

$$R_3(x_1, x_2, x_3) = 1,$$

when $k = 4$

$$\begin{aligned} R_4(x_1, x_2, x_3, x_4) = & 1 - \delta(x_1, x_2) - \delta_2(x_2, x_3) - \delta(x_3, x_4) \\ & - \delta(x_4, x_1) - \delta(x_1, x_3) - \delta(x_2, x_4), \end{aligned}$$

and when $k = 5$

$$\begin{aligned} R_5(x_1, x_2, x_3, x_4, x_5) = & 1 - \sum_{i < j \leq 5} \delta(x_i, x_j) + 2 \sum_{i < j < l \leq 5} \delta(x_i, x_j, x_l) \\ & \sum_{i < j \leq 5} \delta(x_i, x_j) \sum_{\substack{l < m \leq 5 \\ l, m \neq i, j}} \delta(x_l, x_m). \end{aligned}$$

Starting with $k = 5$, there will be terms that are the product of multiple delta functions in multiple variables, and to handle these we need to use the multi-slice rank. Note, for example, that as a function on X^4 ,

$$\delta(x_1, x_2)\delta(x_3, x_4)$$

has slice rank equal to $|X|$ (see [16]) but multi-slice rank equal to 1.

We now use the function $R_p(x_1, \dots, x_p)$ to modify F_p , and arrive at an appropriate tensor.

Lemma 5. *For $x_1, \dots, x_p \in \mathbb{F}_p^n$ define*

$$I_p(x_1, \dots, x_p) = R_p(x_1, \dots, x_p)F_p(x_1, \dots, x_p)$$

where F_p is defined in (3.1) and R_p is defined in 4. Let $B \subset \mathbb{F}_p^n$ be any subset which has no two elements $x, y \in B$ satisfying $x = cy$ for some $c \in \mathbb{F}_p^\times$. Then when restricted to $A^p = A \times \dots \times A$, I_p is given by

$$I_p(x_1, \dots, x_p) = \begin{cases} 1 & \text{if } x_1, \dots, x_p \text{ are distinct and sum to zero} \\ (-1)^{p-1} & \text{if } x_1 = \dots = x_p \\ 0 & \text{otherwise} \end{cases}.$$

Proof. By pairing every element in \mathbb{F}_p^\times with its inverse we have that

$$\sum_{j=2}^{p-1} \frac{1}{j} = -1 + \sum_{j=1}^{p-1} \frac{1}{j} = -1,$$

and so by Wilson's theorem

$$(-1)^{p-1}(p-1)! \sum_{j=2}^{p-1} \frac{1}{j} = (-1)^{p-1},$$

and hence if $x_1 = \dots = x_p$, $I_p(x_1, \dots, x_p) = (-1)^{p-1}$. If there are exactly two distinct elements among x_1, \dots, x_p , say $x, y \in \mathbb{F}_p^n$, then

$$x_1 + \dots + x_p = cx + (p-c)y$$

where $1 \leq c \leq p-1$, and this can never equal 0 by the assumption on B , and so $F_p(x_1, \dots, x_p) = 0$ in this case. When x_1, \dots, x_p are distinct, $F_p(x_1, \dots, x_p) = 1$, and so the result follows. \square

We are now ready to prove theorem 1.

Proof. Suppose that $A \subset \mathbb{F}_p^n$, and that there does not exist distinct $x_1, \dots, x_p \in A$ satisfying

$$x_1 + \dots + x_p = 0.$$

Let $v \in \mathbb{F}_p^n$ be any vector. Then A cannot contain the entire line $0, v, 2v, \dots, (p-1)v$, since this sums to 0, and so A contains at most $p-1$ elements along any line. Thus there exists $B \subset A$ of size

$$|B| \geq \frac{1}{p-1}|A|$$

such that no two elements in B lie on the same line. Since B is a subset of A , there does not exist distinct $x_1, \dots, x_p \in B$ satisfying $x_1 + \dots + x_p = 0$. Letting I_p be defined

as in 5, when we restrict I_p to B^p it will be a diagonal tensor with $(-1)^{p-1}$ along the diagonal, and so by 1

$$|B| \leq \text{multi-slice-rank}(I_p).$$

To bound the multi-slice rank of $I_p(x_1, \dots, x_p)$, consider

$$(3.3) \quad f_\sigma(x_1, \dots, x_p) F_p(x_1, \dots, x_p)$$

where f_σ was defined in (3.2) and F_p was defined in (3.1). We can decompose σ as a product of disjoint cycles $\pi_1 \cdots \pi_t$. Let r_i be the number of elements in the cycle π_i , so that $\sum_{i=1}^t r_i = p$. Write each cycle explicitly as $\pi_i = (j_{i1} \ j_{i2} \ \cdots \ j_{ir_i})$ where j_{il} are indices, and i ranges from 1 to t , and l ranges from 1 to r_i . For $f_\sigma(x_1, \dots, x_p)$ to be non-zero, we must have

$$x_{j_{i1}} = x_{j_{i2}} = \cdots = x_{j_{ir_i}}.$$

Define the function

$$M_{r_1, \dots, r_t}(z_1, \dots, z_t) = \prod_{j=1}^n \left(1 - \left(\sum_{i=1}^t r_i z_{ij} \right)^{p-1} \right).$$

When $f_\sigma = 1$, then we have the equality of functions

$$f_\sigma(x_1, \dots, x_p) F_p(x_1, \dots, x_p) = f_\sigma(x_1, \dots, x_p) M_{r_1, \dots, r_t}(x_{j_{11}}, \dots, x_{j_{t r_t}})$$

and so the multi-slice rank of $f_\sigma(x_1, \dots, x_p) F_p(x_1, \dots, x_p)$ will be at most the slice rank of $M_{r_1, \dots, r_t}(z_1, \dots, z_t)$. This is a polynomial of degree $(p-1)n$ in t variables, and we may expand the product as a linear combination of monomials of the form

$$(z_{11}^{e_{11}} \cdots z_{1n}^{e_{1n}}) (z_{21}^{e_{21}} \cdots z_{2n}^{e_{2n}}) \cdots (z_{t1}^{e_{t1}} \cdots z_{tn}^{e_{tn}}),$$

where $e_{ij} \leq p-1$ and $\sum_{i=1}^t \sum_{j=1}^n e_{ij} \leq (p-1)n$. For each term, there will be some coordinate i such that the monomial

$$z_{i1}^{e_{i1}} \cdots z_{in}^{e_{in}}$$

has degree at most $\frac{(p-1)n}{t}$. By always slicing off the lowest degree piece of our monomial, it follows that the slice rank of M_{r_1, \dots, r_t} will be at most t multiplied by the number of n -variable monomials over \mathbb{F}_p of degree at most $\frac{n(p-1)}{t}$. In other words,

$$(3.4) \quad \text{slice-rank}(M_{r_1, \dots, r_t}) \leq t \cdot \# \left\{ v \in \{0, 1, \dots, p-1\}^n : \sum_{i=1}^n v_i \leq \frac{n(p-1)}{t} \right\}.$$

Let $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$ denote the unsigned Stirling numbers of the first kind, which count the number of elements in S_n which are the product of exactly k disjoint cycles. Thus we have proven that

$$(3.5) \quad \text{multi-slice-rank}(I_p) \leq \sum_{t=3}^p \left[\begin{smallmatrix} n \\ t \end{smallmatrix} \right] t \cdot \# \left\{ v \in \{0, 1, \dots, p-1\}^n : \sum_{i=1}^n v_i \leq \frac{n(p-1)}{t} \right\}.$$

We will use a slightly cruder bound, using the fact that the right hand side of (3.4) as a function of t is largest when $t = 3$. Since there are $p!$ terms, we have the bound

$$\text{multi-slice-rank}(I_p) \leq 3p! \cdot \# \left\{ v \in \{0, 1, \dots, p-1\}^n : \sum_{i=1}^n v_i \leq \frac{n(p-1)}{3} \right\}.$$

Let X_1, \dots, X_n be independent uniform random variables on $\{0, 1, \dots, p-1\}$ and let $X = \sum_{i=1}^n X_i$. Then

$$\# \left\{ v \in \{0, 1, \dots, p-1\}^n : \sum_{i=1}^n v_i \leq \frac{n(p-1)}{3} \right\} \leq p^n \mathbb{P} \left(X \leq \frac{n(p-1)}{3} \right),$$

and we may bound this probability using Markov's inequality, for $0 < x < 1$,

$$\mathbb{P} \left(X \leq \frac{n(p-1)}{3} \right) = \mathbb{P} \left(x^X \geq x^{n(\frac{p-1}{3})} \right) \leq \mathbb{E} (x^X) x^{-n\frac{p-1}{3}}.$$

Since $X = \sum_{i=1}^n X_i$, where each X_i is independent and identically distributed,

$$\begin{aligned} \mathbb{E} (x^X) &= \prod_{i=1}^n \mathbb{E} (x^{X_i}) \\ &= (\mathbb{E} (x^{X_1}))^n \\ &= p^{-n} (1 + x + \dots + x^{p-1})^n \\ &= p^{-n} \left(\frac{1 - x^p}{1 - x} \right)^n, \end{aligned}$$

and so

$$p^n \mathbb{P} \left(X \leq \frac{n(p-1)}{3} \right) \leq \left(\inf_{0 < x < 1} \frac{1 - x^p}{1 - x} x^{-\frac{p-1}{3}} \right)^n.$$

Combining inequalities, we obtain the final result

$$|A| \leq 3(p-1) \cdot p! \left(\min_{0 < x < 1} \frac{1 - x^p}{1 - x} x^{-\frac{p-1}{3}} \right)^n.$$

□

4. CONDITIONAL BOUNDS FOR $s((\mathbb{Z}/k\mathbb{Z})^n)$

The following lemma comes from the proof of proposition 4.14 and theorem 4.15 in [2]:

Lemma 6. *Let q be a prime power. For any $x_1, \dots, x_k \in \mathbb{Z}/q\mathbb{Z}$ we have that*

$$\sum_{m_1 + \dots + m_k \leq q-1} (-1)^{m_1 + \dots + m_k} \binom{x_1}{m_1} \dots \binom{x_k}{m_k} = \begin{cases} 1 & \text{if } x_1 + \dots + x_k = 0 \\ 0 & \text{otherwise} \end{cases}.$$

Proof. This follows since

$$\sum_{m \leq q-1} (-1)^m \binom{x_1 + \dots + x_k}{m} = \begin{cases} 1 & \text{if } x_1 + \dots + x_k = 0 \\ 0 & \text{otherwise} \end{cases},$$

and

$$\binom{x_1 + \dots + x_k}{m} = \sum_{m_1 + \dots + m_k = m} \binom{x_1}{m_1} \dots \binom{x_k}{m_k}.$$

□

We note that the binomial coefficient modulo q is well defined due to Lucas' theorem. For $x_1, \dots, x_k \in (\mathbb{Z}/q\mathbb{Z})^n$ let

$$E_q^k : ((\mathbb{Z}/q\mathbb{Z})^n)^k \rightarrow \mathbb{F}_q$$

be defined by

$$(4.1) \quad E_q^k(x_1, \dots, x_k) = \prod_{i=1}^n \left(\sum_{m_1 + \dots + m_k \leq q-1} (-1)^{m_1 + \dots + m_k} \binom{x_{1i}}{m_1} \dots \binom{x_{ki}}{m_k} \right)$$

where x_{ji} denotes the i^{th} coordinate of the vector x_j . In particular, for $x_1, \dots, x_p \in \mathbb{F}_p^n$, $E_p^p(x_1, \dots, x_p) = F_p(x_1, \dots, x_p)$ where F_p was defined in equation (3.1). For any k, q we have that

$$E_q^k(x_1, \dots, x_k) = \begin{cases} 1 & \text{if } x_1 + x_2 + \dots + x_k = 0 \\ 0 & \text{otherwise} \end{cases},$$

and when $q|k$, $E_q^k(x, \dots, x) = 1$ for any $x \in (\mathbb{Z}/q\mathbb{Z})^n$.

Proposition 1. *The slice-rank of E_q^k on $(\mathbb{Z}/q\mathbb{Z})^n$ is at most $k \cdot \alpha_{k,q}^n$ where*

$$\alpha_{k,q} = \inf_{x>0} \frac{1-x^q}{(1-x)} x^{-\frac{q-1}{k}}.$$

Note in particular that $\alpha_{k,q} = \frac{q}{k} \gamma_{k,q}$.

Proof. Expanding the product form for $E_q^k(x_1, \dots, x_k)$ appearing in (4.1) as a polynomial, we may write $E_q^k(x_1, \dots, x_k)$ as a linear combination of terms of the form

$$\left(\binom{x_{11}}{m_{11}} \dots \binom{x_{1n}}{m_{1n}} \right) \dots \left(\binom{x_{k1}}{m_{k1}} \dots \binom{x_{kn}}{m_{kn}} \right)$$

where $m_{ij} \leq q-1$ for every i, j and

$$\sum_{i=1}^k \sum_{j=1}^n m_{ij} \leq (q-1)n.$$

Thus for each term there is a coordinate i such that

$$\sum_{j=1}^n m_{ij} \leq \frac{(q-1)n}{k},$$

and by always slicing away the lowest degree piece, it follows that

$$(4.2) \quad \text{slice-rank}(E_q^k) \leq k \cdot \# \left\{ v \in \{0, 1, \dots, q-1\}^n : \sum_{i=1}^n v_i \leq \frac{n(q-1)}{k} \right\}.$$

As in the proof of theorem 1, this can be bounded using a Chernoff type technique. Let X_1, \dots, X_n denote independent uniform random variables on $\{0, \dots, q-1\}$, and let $X = \sum_{i=1}^n X_i$. The right hand side of (4.2) is at most

$$q^n \mathbb{P} \left(X \leq \frac{n(q-1)}{k} \right),$$

and by Markov's inequality, for $0 < x < 1$

$$\begin{aligned} \mathbb{P}\left(X \leq \frac{n(q-1)}{k}\right) &\leq \mathbb{E}(x^X) x^{-n\frac{q-1}{k}} \\ &= (\mathbb{E}(x^{X_1}))^n x^{-n\frac{q-1}{k}} \\ &= q^{-n} \left(\frac{1-x^q}{1-x} x^{-\frac{q-1}{k}}\right)^n, \end{aligned}$$

and so we conclude that

$$\text{slice-rank}(E_q^k) \leq k \cdot \left(\min_{0 < x < 1} \frac{1-x^q}{1-x} x^{-\frac{q-1}{k}}\right)^n.$$

□

We now prove theorem 3.

Proof. Let k be given, and let q be the largest prime power dividing k so that $k = qr$. Then

$$(\mathbb{Z}/k\mathbb{Z})^n = (\mathbb{Z}/q\mathbb{Z})^n \times (\mathbb{Z}/r\mathbb{Z})^n$$

where $\gcd(r, q) = 1$. For $x_1 = (g_1, h_1), \dots, x_k = (g_k, h_k) \in (\mathbb{Z}/q\mathbb{Z})^n \times (\mathbb{Z}/r\mathbb{Z})^n$ define

$$J_k : ((\mathbb{Z}/k\mathbb{Z})^n)^k \rightarrow \mathbb{F}_q$$

by

$$J_k(x_1, \dots, x_k) = E_q^k(g_1, \dots, g_k)W(h_1, \dots, h_k)$$

where W is the function

$$W(h_1, \dots, h_k) = \begin{cases} 1 & \text{if } h_1 + \dots + h_k = 0 \\ 0 & \text{otherwise} \end{cases}.$$

Suppose that $A \subset (\mathbb{Z}/k\mathbb{Z})^n$ does not contain a non-trivial k -tuple that sums to zero. Then when restricted to A^k , J_k will be a diagonal tensor taking the value 1 on the diagonal. Hence lemma 1 implies that

$$|A| \leq \text{slice-rank}(J_k).$$

By lemma 2,

$$\text{slice-rank}(J_k) \leq r^n \cdot \text{slice-rank}(E_q^k),$$

and hence by proposition 1 it follows that

$$\begin{aligned} |A| &\leq k \cdot r^n \cdot \left(\min_{0 < x < 1} \frac{1-x^q}{1-x} x^{-\frac{q-1}{k}}\right)^n \\ &= k \cdot \left(\frac{k}{q} \min_{0 < x < 1} \frac{1-x^q}{1-x} x^{-\frac{q-1}{k}}\right)^n \\ &= k \cdot \gamma_{k,q}^n. \end{aligned}$$

We can remove the factor of k using a standard amplification argument. If $A \subset (\mathbb{Z}/k\mathbb{Z})^n$ does not contain a non-trivial k -tuple that sums to zero, then the m -fold Cartesian product $A^m = A \times \dots \times A$ viewed as a subset of $(\mathbb{Z}/k\mathbb{Z})^{nm}$ will not contain a non-trivial k -tuple summing to 0, and so

$$|A|^m \leq k \cdot \gamma_{k,q}^{nm}$$

and

$$|A| \leq k^{\frac{1}{m}} \gamma_{k,q}^n.$$

Letting $m \rightarrow \infty$, we obtain theorem 3. □

5. FUTURE WORK AND DISCUSSION OF RESULTS

Theorem 1 does not seem to extend to give unconditional bounds on $s((\mathbb{Z}/k\mathbb{Z})^n)$. The multi-slice rank method fails to handle $(\mathbb{Z}/k\mathbb{Z})^n$, and this is due to two major obstructions:

Obstruction 1: The first problem is that we cannot extend from $(\mathbb{Z}/p\mathbb{Z})^n$ to $(\mathbb{Z}/q\mathbb{Z})^n$ where $q = p^r$, $r > 1$, by using the binomial coefficients as indicator functions, as was done in the proof of theorem 3. The issue is that the indicator function $R_q(x_1, \dots, x_q)$, which captures whether or not the variables will be distinct, satisfies

$$R_q(x_1, \dots, x_q) = (-1)^{q-1}(q-1)! \sum_{j=2}^{q-1} \frac{1}{j}$$

when $x_1 = \dots = x_q$. For $r > 1$, this will be 0 modulo p , and so our indicator tensor will take 0 on the diagonal, and this causes the method to fail.

Obstruction 2: The second problem is more severe. In the proof of theorem 3, to extend to products of primes we took insight from [2], and used lemma 2, which gave a bound on the slice rank of a tensor product. For a k -dimensional tensor $u \otimes v$ on $(G \times H)^k$ lemma 2 states that

$$\text{slice-rank}(u \otimes v) \leq \text{slice-rank}(u) \cdot |H|,$$

and to extend theorem 1 to products of primes, we would need a version of lemma 2 for the multi-slice rank. However such a result does not seem to hold. Working through the proof of lemma 2, we find that a b -slice will pick up a factor of $|H|^b$ instead of just a factor of $|H|$, and this leads to the significantly weaker bound

$$\text{multi-slice-rank}(u \otimes v) \leq \text{multi-slice-rank}(u) |H|^{\lfloor \frac{k}{2} \rfloor}.$$

Acknowledgements

I would like to thank Will Sawin for helpful discussions and for his simple proof of lemma 3. This work was partially supported by the NSERC PGS-D scholarship, and by Ben Green's ERC Starting Grant 279438, Approximate Algebraic Structure and Applications.

REFERENCES

1. N. Alon and M. Dubiner, *Zero-sum sets of prescribed size*, Combinatorics, Paul Erdős is eighty, Vol. 1, Bolyai Soc. Math. Stud., János Bolyai Math. Soc., Budapest, 1993, pp. 33–50. MR 1249703
2. Jonah Blasiak, Thomas Church, Henry Cohn, Joshua Grochow, Eric Naslund, William F. Sawin, and Christopher Umans, *On cap sets and the group-theoretic approach to matrix multiplication*, preprint, 2016, arXiv:1605.06702.
3. Ernie Croot, Vsevolod Lev, and Peter Pach, *Progression-free sets in \mathbb{Z}_4^n are exponentially small*, Ann. of Math. (2) **185** (2017), 331–337, arXiv:1605.01506, doi:10.4007/annals.2017.185.1.7.
4. Jordan Ellenberg and Dion Gijswijt, *On large subsets of \mathbb{F}_q^n with no three-term arithmetic progression*, Ann. of Math. (2) **185** (2017), 339–343, arXiv:1605.09223, doi:10.4007/annals.2017.185.1.8.
5. Paul Erdos, Abraham Ginzburg, and Abraham Ziv, *A theorem in additive number theory*, Bull. Res. Council Israel **10F** (1961), 41–43.
6. Paul Erdős and Endre Szemerédi, *Combinatorial properties of systems of sets*, J. Combinatorial Theory Ser. A **24** (1978), 308–313, doi:10.1016/0097-3165(78)90060-2.
7. Weidong Gao and Alfred Geroldinger, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), no. 4, 337–369. MR 2313123

8. Heiko Harborth, *Ein Extremalproblem für Gitterpunkte*, J. Reine Angew. Math. **262/263** (1973), 356–360, Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday. MR 0327666
9. Gábor Hegedüs, *The Erdős-Ginzburg-Ziv constant and progression-free subsets*, preprint, 2017, arXiv:1701.01038.
10. Arnfried Kemnitz, *On a lattice point problem*, Ars Combin. **16** (1983), no. B, 151–160. MR 737118
11. Alfred Geroldinger and Franz Halter-Koch, *Non-unique factorizations*, Pure and Applied Mathematics (Boca Raton), vol. 278, Chapman & Hall/CRC, Boca Raton, FL, 2006, Algebraic, combinatorial and analytic theory. MR 2194494
12. Eric Naslund, *The multi-slice rank method and polynomial bounds for orthogonal systems in \mathbb{F}_q^n* , preprint, 2017, arXiv:1701.04475.
13. Eric Naslund and William F. Sawin, *Upper bounds for sunflower-free sets*, preprint, 2016, arXiv:1606.09575.
14. Christian Reiher, *On Kemnitz' conjecture concerning lattice-points in the plane*, Ramanujan J. **13** (2007), no. 1-3, 333–337. MR 2281170
15. Terence Tao, A symmetric formulation of the Croot–Lev–Pach–Ellenberg–Gijswijt capset bound, blog post, 2016, <http://terrytao.wordpress.com/2016/05/18/a>.
16. Terence Tao and William F. Sawin, Notes on the "slice rank" of tensors, blog post, 2016, <https://terrytao.wordpress.com/2016/08/24/notes-on-the-slice-rank-of-tensors/>.